CLAIMS

What is claimed is:

1. A method for effecting a chained key-issuing process over a finite group of points in which the discrete logarithm problem applies, wherein an issuing user ($User_i$), who possesses an issuing user public value ($\mathbf{U}_i$) and an issuing user private key (x_i), provides to a successor user ($User_{(i+1)}$) a successor user public value ($\mathbf{U}_{(i+1)}$) and a successor user private key ($x_{(i+1)}$), and where said issuing user, except for a Certifying Authority (CA), was a successor user in a preceding step in the chained key-issuing process, and where said Certifying Authority acts as the first issuing user in the chained key-issuing process, said method comprising the steps of:

(a) permitting said Certifying Authority to select a generating group-point ($\mathbf{G}$) whose exponentiations to various powers generate various group-points and a converting mathematical operation (H) which converts several input values into a scalar;

(b) permitting said Certifying Authority to posses a Certifying Authority private key (x_0);

(c) permitting said Certifying Authority to posses a Certifying Authority public value ($\mathbf{U}_0$), obtained by exponentiating said generating group-point to the power of said Certifying Authority private key ($\mathbf{U}_0 = x_0 * \mathbf{G}$);

(d) permitting said issuing user ($User_i$) to possess said generating group-point ($\mathbf{G}$) and said converting mathematical operation (H) and the identification details ($ID_{(i+1)}$) of said successor user;

(e) permitting said issuing user ($User_i$) to possess an issuing user private key (x_i), where, except for the case in which said issuing user is said Certifying Authority, said

issuing user private key was provided to said issuing user at a preceding stage in the chained key-issuing process (in which Useri acted as a successor user in respect to an issuing User(i-1));

(f) permitting said issuing user (Useri) to calculate said successor user public value ($\mathbf{U_{(i+1)}}$) and said successor user private key ($x_{(i+1)}$) wherein:

a successor user random value ($k_{(i+1)}$) is generated and said successor user public value ($\mathbf{U_{(i+1)}}$) is calculated by exponentiating said generating group-point to the power of said successor user random value ($\mathbf{U_{(i+1)}} = k_{(i+1)} * \mathbf{G}$);

a successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) is calculated by operating with said converting mathematical operation on said successor user identification details ($ID_{(i+1)}$) and said successor user public value ($\mathbf{U_{(i+1)}}$);

said successor user private key ($x_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) by said successor user random value ($k_{(i+1)}$) and adding said issuing user private key (x_i) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}}) * k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point; and

(g) permitting said issuing user (Useri) to submit said successor user public value ($\mathbf{U_{(i+1)}}$) and said successor user private key ($x_{(i+1)}$) to said successor user ($User_{(i+1)}$).

2. A method for effecting a chained key-issuing process as recited in claim 1, where the issuing user (Useri) does not know the successor user private key ($x_{(i+1)}$), said method further comprising the steps of:

permitting said successor user ($User_{(i+1)}$) to generate a first random value ($m_{(i+1)}$) and calculate a first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) by exponentiating the generating group-point to the power of said first random value;

permitting said successor user to submit said first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) to said issuing user ($User_i$);

permitting said issuing user to calculate a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user intermediate private key ($p_{(i+1)}$), wherein:

a second random value ($k_{(i+1)}$) is generated and a second intermediate group-point ($k_{(i+1)}*\mathbf{G}$) is calculated by exponentiating said generating group-point to the power of said second random value;

said successor user public value ($\mathbf{U_{(i+1)}}$) is calculated by adding said first intermediate group-point and said second intermediate group-point ($\mathbf{U_{(i+1)}} = m_{(i+1)}*\mathbf{G} + k_{(i+1)}*\mathbf{G}$);

a successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) is calculated in the way described;

said successor user intermediate private key ($p_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) by said second random value ($k_{(i+1)}$) and adding the issuing user private key (x_i) to the product obtained by said multiplication ($p_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point; and

permitting said successor user to generate the successor user private key ($x_{(i+1)}$) by calculating said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) in the way described and

multiplying said successor user representing value by said first random value ($m_{(i+1)}$) and adding said successor user intermediate private key ($p_{(i+1)}$) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*m_{(i+1)} + p_{(i+1)}$) and reducing the result modulo the order of said generating group-point.

3. A certificate generation system for permitting a generating user who is a successor user ($User_{(i+1)}$) to issue a certificate to a general user ($User_{(i+2)}$) where said certificate attests to the association between said general user public key ($\mathbf{Y_{(i+2)}}$) and said general user identification details ($ID_{(i+2)}$), where said general user public key was issued to said general user according to any known public key cryptographic method, wherein an issuing user ($User_i$), who possesses an issuing user public value ($\mathbf{U_i}$) and an issuing user private key (x_i), provides to a successor user ($User_{(i+1)}$) a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user private key ($x_{(i+1)}$), and where said issuing user, except for a Certifying Authority (CA), was a successor user in a preceding step in the chained key-issuing process, and where said Certifying Authority acts as the first issuing user in the chained key-issuing process, said system comprising:

means for permitting said generating user to generate a first random scalar ($k_{(i+2)}$);

means for permitting said generating user to calculate a first part of a certificate ($\mathbf{T_{(i+2)}}$) by exponentiating the generating group-point to the power of said first random scalar ($\mathbf{T_{(i+2)}} = k_{(i+2)}*\mathbf{G}$);

means for permitting said generating user to calculate a general user representing value ($H(ID_{(i+2)},\mathbf{Y_{(i+2)}},\mathbf{T_{(i+2)}})$) by operating with the converting mathematical operation on said

general user identification details ($ID_{(i+2)}$) and said general user public key ($\mathbf{Y_{(i+2)}}$) and said first part of a certificate ($\mathbf{T_{(i+2)}}$);

means for permitting said generating user to calculate a second part of a certificate ($s_{(i+2)}$) by multiplying said general user representing value by said first random scalar ($k_{(i+2)}$) and adding the private key ($x_{(i+1)}$) of said generating user to the product obtained by said multiplication ($s_{(i+2)} = H(ID_{(i+2)},\mathbf{Y_{(i+2)}},\mathbf{T_{(i+2)}})*k_{(i+2)} + x_{(i+1)}$) and reducing the result modulo the order of said generating group-point; and

means for permitting said generating user to submit said certificate to said general user, said certificate comprising of said first part of a certificate ($\mathbf{T_{(i+2)}}$) and said second part of a certificate ($s_{(i+2)}$).

4. A chained certificate verification system for permitting a verifying user to verify the authenticity of a certificate ($\mathbf{T_{(i+2)}}$ and $s_{(i+2)}$) issued to a general user ($User_{(i+2)}$) where said certificate attests to the association between said general user public key ($\mathbf{Y_{(i+2)}}$) and said general user identification details ($ID_{(i+2)}$), where said general user public key was issued to said general user according to any known public key cryptographic method, the system comprising:

means for providing said verifying user with said certificate and with the general user public key ($\mathbf{Y_{(i+2)}}$) and with the general user identification details ($ID_{(i+2)}$) and with the Certifying Authority public value ($\mathbf{U_0}$) and with a plurality of pairs of values (ID_j and $\mathbf{U_j}$) consisting of the identification details and public values of all users ($User_j$, $j = 1, 2,\ldots, i+1$)) in the chained key-issuing process over a finite group of points in which the discrete logarithm problem applies, wherein an issuing user ($User_i$), who possesses an issuing user public value ($\mathbf{U_i}$)

and an issuing user private key (x_i), provides to a successor user ($User_{(i+1)}$) a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user private key ($x_{(i+1)}$), and where said issuing user, except for a Certifying Authority (CA), was a successor user in a preceding step in the chained key-issuing process, and where said Certifying Authority acts as the first issuing user in the chained key-issuing process, starting with the first successor user ($User_1$) after the Certifying Authority and ending with the successor user ($User_{(i+1)}$);

means for permitting said verifying user to verify the validity of said certificate, wherein:

a first scalar ($H(ID_{(i+2)},\mathbf{Y_{(i+2)}},\mathbf{T_{(i+2)}})$) is calculated by operating with the converting mathematical operation on said general user identification details ($ID_{(i+2)}$) and said general user public key ($\mathbf{Y_{(i+2)}}$) and the first part of said certificate ($\mathbf{T_{(i+2)}}$);

a first intermediate group-point ($H(ID_{(i+2)},\mathbf{Y_{(i+2)}},\mathbf{T_{(i+2)}})*\mathbf{T_{(i+2)}}$) is calculated by exponentiating said first part of the certificate ($\mathbf{T_{(i+2)}}$) to the power of said first scalar;

users representing values ($H(ID_j,\mathbf{U_j})$, $j = 1, 2,\ldots, i+1$) are calculated by operating with said converting mathematical operation on each pair of said plurality of pairs of values (ID_j and $\mathbf{U_j}$);

users temporary group-points ($H(IDj,\mathbf{U_j})*\mathbf{U_j}$, $j = 1, 2,\ldots, i+1$) are calculated for each user in said chained key-issuing process, starting with said first successor user ($User_1$) and ending with said generating user ($User_{(i+1)}$), by exponentiating each said user public value ($\mathbf{U_j}$) to the power of said user representing value ($H(ID_j,\mathbf{U_j})$);

a second intermediate group-point (**P**) is calculated by adding all said users temporary group-points ($\mathbf{P} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*\mathbf{U_{(i+1)}} + H(IDi,\mathbf{Ui})*\mathbf{Ui} + H(ID_{(i-1)},\mathbf{U_{(i-1)}})*\mathbf{U_{(i-1)}} + \ldots + H(ID_1,\mathbf{U_1})*\mathbf{U_1}$);

a third intermediate group-point (**Q**) is calculated by adding said first intermediate group-point and said second intermediate group-point and the public value of said Certifying Authority ($\mathbf{Q} = H(ID_{(i+2)},\mathbf{Y_{(i+2)}},\mathbf{T_{(i+2)}})*\mathbf{T_{(i+2)}} + \mathbf{P} + \mathbf{U_0}$);

a fourth intermediate group-point ($s_{(i+2)}*\mathbf{G}$) is calculated by exponentiating the generating group-point to the power of the first part ($s_{(i+2)}$) of said certificate;

the value of said fourth intermediate group-point ($s_{(i+2)}*\mathbf{G}$) is compared to that of said third intermediate group-point (**Q**) and the certificate is determined as being valid in the case of equality.

5. A chained signature generation and verification system for permitting a successor user ($User_{(i+1)}$) to generate a signature and permitting a verifying party to verify said signature, wherein an issuing user ($User_i$), who possesses an issuing user public value (**Ui**) and an issuing user private key (x_i), provides to a successor user ($User_{(i+1)}$) a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user private key ($x_{(i+1)}$), and where said issuing user, except for a Certifying Authority (CA), was a successor user in a preceding step in a chained key-issuing process, and where said Certifying Authority acts as the first issuing user in the chained key-issuing process, the system comprising:

means for permitting said successor user ($User_{(i+1)}$) to generate a signature on a message (m) wherein:

a first scalar (k) is randomly generated;

a first part of a signature (**T**) is generated by exponentiating the generating group-point to the power of said first scalar ($\mathbf{T} = k*\mathbf{G}$);

a representing value ($H(m,\mathbf{T})$) is generated by operating with the converting mathematical operation on said message (m) and said first part of a signature (**T**);

a second part of a signature (s) is calculated by multiplying said representing value ($H(m,\mathbf{T})$) by said first scalar (k) and adding the private key of said successor user ($x_{(i+1)}$) to the product obtained by said multiplication ($s = H(m,\mathbf{T})*k + x_{(i+1)}$) and reducing the result modulo the order of said generating group-point;

means for permitting said successor user to submit said message (m) and said signature (**T** and s) to said verifying party, said signature comprising of said first part of a signature (**T**) and said second part of a signature (s);

means for providing said verifying party with the Certifying Authority public value ($\mathbf{U_0}$) and with a plurality of pairs of values (ID_j and $\mathbf{U_j}$) consisting of the identification details and public values (ID_j and $\mathbf{U_j}$) of all users ($User_j$, $j = 1, 2,\ldots, i+1$)) in the chained key-issuing process, starting with the first successor user ($User_1$) after the Certifying Authority and ending with said successor user ($User_{(i+1)}$);

means for permitting said verifying party to verify the validity of said signature (**T** and s) on said message (m), wherein:

said representing value ($H(m,\mathbf{T})$) is generated in the way described;

a first intermediate group-point ($H(m,\mathbf{T})*\mathbf{T}$) is calculated by exponentiating said first part of the signature ($\mathbf{T}$) to the power of said representing value;

users representing values ($H(ID_j,\mathbf{U_j})$, $j = 1, 2,\ldots, i+1$) are calculated by operating with said converting mathematical operation on each pair of said plurality of pairs of values (ID_j and $\mathbf{U_j}$);

users temporary group-points ($H(IDj,\mathbf{U_j})*\mathbf{U_j}$, $j = 1, 2,\ldots, i+1$) are calculated for each user in said chained key-issuing process, starting with said first successor user ($User_1$) and ending with said successor user ($User_{(i+1)}$), by exponentiating each said user public value ($\mathbf{U_j}$) to the power of said user representing value ($H(ID_j,\mathbf{U_j})$);

a second intermediate group-point ($\mathbf{P}$) is calculated by adding all said temporary group-points ($\mathbf{P} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*\mathbf{U_{(i+1)}} + H(IDi,\mathbf{U_i})*\mathbf{U_i} + H(ID_{(i-1)},\mathbf{U_{(i-1)}})*\mathbf{U_{(i-1)}} + \ldots + H(ID_1,\mathbf{U_1})*\mathbf{U_1}$);

a third intermediate group-point ($\mathbf{Q}$) is calculated by adding said first intermediate group-point and said second intermediate group-point and the public value of said Certifying Authority ($\mathbf{Q} = H(m,\mathbf{T})*\mathbf{T} + \mathbf{P} + \mathbf{U_0}$);

a fourth intermediate group-point ($s*\mathbf{G}$) is calculated by exponentiating the generating group-point to the power of the first part (s) of said signature;

the value of said fourth intermediate group-point ($s*\mathbf{G}$) is compared to that of said third intermediate group-point ($\mathbf{Q}$) and the signature is determined as being valid in the case of equality.

6. A chained signature generation and verification system as recited by claim 5, wherein the chained-key issuing process comprises the steps of:

(a) permitting said Certifying Authority to select a generating group-point (**G**) whose exponentiations to various powers generate various group-points and a converting mathematical operation (H) which converts several input values into a scalar;

(b) permitting said Certifying Authority to posses a Certifying Authority private key (x_0);

(c) permitting said Certifying Authority to posses a Certifying Authority public value ($\mathbf{U_0}$), obtained by exponentiating said generating group-point to the power of said Certifying Authority private key ($\mathbf{U_0} = x_0 * \mathbf{G}$);

(d) permitting said issuing user ($User_i$) to possess said generating group-point (**G**) and said converting mathematical operation (H) and the identification details ($ID_{(i+1)}$) of said successor user;

(e) permitting said issuing user ($User_i$) to possess an issuing user private key (x_i), where, except for the case in which said issuing user is said Certifying Authority, said issuing user private key was provided to said issuing user at a preceding stage in the chained key-issuing process (in which $User_i$ acted as a successor user in respect to an issuing $User_{(i-1)}$);

(f) permitting said issuing user ($User_i$) to calculate said successor user public value ($\mathbf{U_{(i+1)}}$) and said successor user private key ($x_{(i+1)}$) wherein:

a successor user random value ($k_{(i+1)}$) is generated and said successor user public value ($\mathbf{U_{(i+1)}}$) is calculated by exponentiating said generating group-point to the power of said successor user random value ($\mathbf{U_{(i+1)}} = k_{(i+1)}*\mathbf{G}$);

a successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) is calculated by operating with said converting mathematical operation on said successor user identification details ($ID_{(i+1)}$) and said successor user public value ($\mathbf{U_{(i+1)}}$);

said successor user private key ($x_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) by said successor user random value ($k_{(i+1)}$) and adding said issuing user private key (x_i) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point; and

(g) permitting said issuing user ($User_i$) to submit said successor user public value ($\mathbf{U_{(i+1)}}$) and said successor user private key ($x_{(i+1)}$) to said successor user ($User_{(i+1)}$).

7. A certificate generation system as recited by claim 3, wherein the successor user ($User_{(i+1)}$) is defined according to a method comprising the steps of:

permitting said successor user ($User_{(i+1)}$) to generate a first random value ($m_{(i+1)}$) and calculate a first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) by exponentiating the generating group-point to the power of said first random value;

permitting said successor user to submit said first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) to said issuing user ($User_i$);

permitting said issuing user to calculate a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user intermediate private key ($p_{(i+1)}$), wherein:

a second random value ($k_{(i+1)}$) is generated and a second intermediate group-point ($k_{(i+1)}*\mathbf{G}$) is calculated by exponentiating said generating group-point to the power of said second random value;

said successor user public value ($\mathbf{U_{(i+1)}}$) is calculated by adding said first intermediate group-point and said second intermediate group-point ($\mathbf{U_{(i+1)}} = m_{(i+1)}*\mathbf{G} + k_{(i+1)}*\mathbf{G}$);

a successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) is calculated in the way described;

said successor user intermediate private key ($p_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) by said second random value ($k_{(i+1)}$) and adding the issuing user private key (x_i) to the product obtained by said multiplication ($p_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point; and

permitting said successor user to generate the successor user private key ($x_{(i+1)}$) by calculating said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) in the way described and multiplying said successor user representing value by said first random value ($m_{(i+1)}$) and adding said successor user intermediate private key ($p_{(i+1)}$) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*m_{(i+1)} + p_{(i+1)}$) and reducing the result modulo the order of said generating group-point.

8. A chained certificate verification system as recited by claim 4, wherein the chained key-issuing process is defined according to a method comprising the steps of:

permitting said successor user ($User_{(i+1)}$) to generate a first random value ($m_{(i+1)}$) and calculate a first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) by exponentiating the generating group-point to the power of said first random value;

permitting said successor user to submit said first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) to said issuing user ($User_i$);

permitting said issuing user to calculate a successor user public value ($\mathbf{U}_{(i+1)}$) and a successor user intermediate private key ($p_{(i+1)}$), wherein:

a second random value ($k_{(i+1)}$) is generated and a second intermediate group-point ($k_{(i+1)}*\mathbf{G}$) is calculated by exponentiating said generating group-point to the power of said second random value;

said successor user public value ($\mathbf{U}_{(i+1)}$) is calculated by adding said first intermediate group-point and said second intermediate group-point ($\mathbf{U}_{(i+1)} = m_{(i+1)}*\mathbf{G} + k_{(i+1)}*\mathbf{G}$);

a successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) is calculated in the way described;

said successor user intermediate private key ($p_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) by said second random value ($k_{(i+1)}$) and adding the issuing user private key (x_i) to the product obtained by said

multiplication ($p_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point; and

permitting said successor user to generate the successor user private key ($x_{(i+1)}$) by calculating said successor user representing value ($H(ID_{(i+1)},\mathbf{U_{(i+1)}})$) in the way described and multiplying said successor user representing value by said first random value ($m_{(i+1)}$) and adding said successor user intermediate private key ($p_{(i+1)}$) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*m_{(i+1)} + p_{(i+1)}$) and reducing the result modulo the order of said generating group-point.

8. A chained signature generation and verification system as recited by claim 5, wherein the successor user ($User_{(i+1)}$) is defined according to a method comprising the steps of:

permitting said successor user ($User_{(i+1)}$) to generate a first random value ($m_{(i+1)}$) and calculate a first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) by exponentiating the generating group-point to the power of said first random value;

permitting said successor user to submit said first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) to said issuing user ($User_i$);

permitting said issuing user to calculate a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user intermediate private key ($p_{(i+1)}$), wherein:

a second random value ($k_{(i+1)}$) is generated and a second intermediate group-point ($k_{(i+1)}*\mathbf{G}$) is calculated by exponentiating said generating group-point to the power of said second random value;

said successor user public value ($\mathbf{U}_{(i+1)}$) is calculated by adding said first intermediate group-point and said second intermediate group-point ($\mathbf{U}_{(i+1)} = m_{(i+1)} * \mathbf{G} + k_{(i+1)} * \mathbf{G}$);

a successor user representing value ($H(ID_{(i+1)}, \mathbf{U}_{(i+1)})$) is calculated in the way described;

said successor user intermediate private key ($p_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)}, \mathbf{U}_{(i+1)})$) by said second random value ($k_{(i+1)}$) and adding the issuing user private key (x_i) to the product obtained by said multiplication ($p_{(i+1)} = H(ID_{(i+1)}, \mathbf{U}_{(i+1)}) * k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point; and

permitting said successor user to generate the successor user private key ($x_{(i+1)}$) by calculating said successor user representing value ($H(ID_{(i+1)}, \mathbf{U}_{(i+1)})$) in the way described and multiplying said successor user representing value by said first random value ($m_{(i+1)}$) and adding said successor user intermediate private key ($p_{(i+1)}$) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)}, \mathbf{U}_{(i+1)}) * m_{(i+1)} + p_{(i+1)}$) and reducing the result modulo the order of said generating group-point.